REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is made obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-6, 8-23, 25-40 AND 42-51 UNDER 35 U.S.C. §103

Claims 1-6, 8-23, 25-40 and 42-51 stand rejected as being unpatentable over the Bots et al. patent (United States Patent No. 6,226,748, issued May 1, 2001, hereinafter "Bots") in view of the Pandya et al. patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya") and further in view of the Li patent (United States Patent No. 6,751,220, issued June 15, 2004, hereinafter "Li"). In response, the Applicants have amended independent claims 1, 18 and 35, from which claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 depend, in order to more clearly recite aspects of the present invention. Claims 2, 19, and 36 have been cancelled without prejudice.

Particularly, the Examiner's attention is directed to the fact that Bots, Pandya, and Li, singly or in any permissible combination, fail to disclose or suggest the novel invention of a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes and can perform a membership change in an associated subset without notifying all of the other master nodes of the change, as claimed in Applicants' amended independent claims 1, 18 and 35.

By contrast, Bots teaches that the VPN units (VPNUs) (which the Examiner equates with "master nodes") use lookup tables in order to determine whether source and destination addresses are members of the same VPN group. These lookup tables must be consistent from VPNU to VPNU in order for messages to be handled properly: "It is assumed that the lookup tables maintained by all of the VPN units are both consistent and coherent" (Bots, col. 7, ll. 63-65, emphasis added). If all VPNUs must have the same global view of the network, then it is impossible for a VPNU to make a membership change without informing the other VPNUs. That is, when a VPNU makes a membership change, it must update the lookup table, thereby necessarily informing

the other VPNUs of the membership change.

Likewise, Pandya teaches that a control point (which the Examiner equates with a "master node") "includes a synchronization interface (not shown) for synchronizing information among multiple control points within the same domain" (Pandya, col. 20, ll. 24-26, emphasis added). Again, if the control points are required to share a globally consistent view of the network, then they cannot make changes without informing the other control points.

Li, similar to Bots, also teaches storing VPN data "from many different VPNs ... in a single routing table" (Li, col. 2, ll. 57-59, emphasis added). If the VPNs share the routing table, then any change made to the routing table by one VPN will necessarily be available to other VPNs that use the routing table. Thus, a VPN cannot perform a membership change in Li's system without informing the other VPNs that share the routing table of the change.

Notably, Applicants' invention positively claims master nodes that control admission and departure in a VPN for an associated non-empty subset of member nodes and that can perform a membership change in an associated subset without notifying all of the other master nodes of the change, as claimed in Applicants' amended independent claims 1, 18 and 35. Specifically, Applicants' claims 1, 18 and 35, as amended, positively recite:

1. A group management system comprising:

a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted by said interconnected nodes; and

a plurality of master nodes, different from the plurality of interconnected nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes,

wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset. (Emphasis added)

18. A method for managing a group, the method comprising:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted by said interconnected nodes; and

providing a plurality of master nodes, different from the plurality of interconnected nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes,

wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset. (Emphasis added)

35. A computer readable medium containing an executable program for managing a group, where the program performs the steps of:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted by said interconnected nodes; and

providing a plurality of master nodes, different from the plurality of interconnected nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes,

wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset. (Emphasis added)

The Applicants' invention is directed to systems and methods for scalable distributed management of virtual private networks (VPNs). The management of encrypted group communications necessary to establish secure, private VPN communications channels through an underlying public network infrastructure places a variety of burdens on a VPN manager. In particular, the addition or removal of a member from a VPN often involves the generation and distribution of one or more new encryption keys that allow current VPN members to decrypt private communications

sent through the VPN, but prevent non-VPN members from decrypting the communications. As VPN membership increases and changes dynamically with greater frequency, the complexity of encryption key management becomes even more burdensome. Thus, the VPN manager becomes a single point of failure for the entire VPN; overload of the VPN manager can cause the entire VPN to fail. This makes the VPN architecture very difficult and very costly to scale, which is not ideal for enterprises relying on secure and private electronic communications.

The Applicants' invention enhances the scalability of a VPN by dividing the member nodes of the VPN into subsets and providing a plurality of master nodes that are each associated with a subset of member nodes to control membership (*i.e.*, admission and departure) in the VPN and to facilitate VPN communications for that subset. For example, each master node is responsible for managing the generation and distribution of encryption keys for only its associated subset(s), so that VPN communication and management burdens are not placed entirely on a single master node. By this scheme, it is unnecessary for a master node, having performed a membership change in its associated subset of member nodes, to inform the other master nodes not associated with the changed subset of this membership change. This renders the VPN architecture more easily scalable than a VPN employing a more conventional architecture, because a plurality of new member nodes may be added or admitted to the VPN through a discrete master node, without the need to regenerate or redistribute encryption keys to all member nodes in the entire VPN.

The Applicants' invention positively claims that a master node can perform a membership change in an associated subset of member nodes without notifying all of the other master nodes of the change. As described above, Bots, Pandya, and Li, singly or in any permissible combination, fail to teach or suggest a mechanism by which a master node can perform a membership change in an associated subset of member without notifying all of the other master nodes of the change, but rather teach that the equivalents of "master nodes" must share a globally consistent view of network membership in order for network communications to operate properly.

Bots, Pandya, and Li thus fail to teach or anticipate a virtual private network

(VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes and can perform a membership change in an associated subset without notifying all of the other master nodes of the change, as positively claimed by the Applicants in amended claims 1, 18 and 35. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35, as amended, fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 are not made obvious by the teachings of Bots in view of Pandya and further in view of Li. Therefore, the Applicants submit that dependent claims 3-6, 8-17, 20-23, 25-34, 37-40 and 42-51 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

II. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

09/844,693

Respectfully submitted,

10/30/07
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702